Trusted Product Efforts in the U.S. and Abroad

This module describes the various trusted product efforts that aretaking place in the U.S. and in various international communities. It defines the concepts of evaluation, certification and accreditation to address potentialconfusion and to provide understanding about the role of evaluated products. It describes national efforts in the areas of criteria development and evaluationprocesses , and mentions export controls that could have a significant bearing on a product's market niche. It also introduces the international organizations involved in trusted product efforts abroad. It concludes with a discussion of work to harmonize the various evaluation criteria that exist internationally.

Module Learning Objectives

This module presents material that can be read independently of theother modules. Upon completion of this module, the student should:

1. Be aware of the evaluation/certification/accreditation process.
2. Be aware of national efforts to advance evaluation criteria and evaluation processes.
3. Be aware of international efforts going on in these areas.
4. Be aware of the U.S. government's export controls on trusted systems and components.

Overview

This course has been developed to assist vendors who are preparing to participate in the TPEP process conducted by NSA. However, there are many other efforts related to fielding trusted products that exist in the U.S. and abroad. This module provides the reader with a broad perspective ofon-going trusted product efforts and how TPEP fits in.

In order to understand the different efforts and how they relate, it is important to first define three basic concepts: evaluation, certification,and accreditation. After describing these concepts, this module provides an overview of applicable trusted product efforts taking place in the U.S. The module then describes on-going international efforts, and concludes with the status of an effort to develop a common (harmonized) set of evaluation criteria.

Evaluation, Certification, and Accreditation

The terms "evaluation," "certification" and "accreditation" can becomeconfused because they are frequently used interchangeably even though they have distinct meanings. The confusion is compounded by the fact that the same term may have different meanings from one organization to the next. This section defines the three terms to help shed some light on the role ofevaluated products in the U.S and abroad.

Evaluation

In the U.S., an evaluation is a technical analysis of a *product's* protection features, independent of any mission or operational environment, against a

stated criteria. Such evaluations are principally performed by NSA on commercial "off-the-shelf" products through TPEP, and culminate with an entry on the Evaluated Products List (EPL). The completion of anevaluation does not constitute approval for the product to be used in anyspecific environment. On the contrary, the certification and accreditation procedures must still be followed before a product can be approved for use inprocessing U.S. government classified information. The results of a product evaluation are typically used as input during the certification process. This input is intended to make certification more efficient since the security features ofevaluated products, unless modified, do not have to be repeatedly examined in-depth.

In Europe, technical security analysis is performed by the vendor; evaluators review the vendor's security analysis and document their findings in a report that is submitted to a certifier. Evaluations are performed by commercially licensed evaluation facilities (CLEFs) on both products and systems, where a *product* is evaluated independent of its environment and a *system* comprises products in conjunction with custom-made code developed for a specific environment.

Certification

In the U.S., certification is a technical assessment of the ability of a *procedure, program*, *system component*, or *system* to meet its mission requirements in a particular operational environment. It culminates with the issuance of certification statements that indicate the degree of compliance with aset of pre-specified security requirements and that identify all knownremaining vulnerabilities. All certification documentation is provided as input to the accreditation process. [ACAP92] gives an example of the technical analysis required to support the certification of controlled access protectionin AISs submitted for accreditation.

In Europe, a certifier is responsible for overseeing work done by commercial evaluators to ensure consistency among evaluations and to develop a "certification report" based on findings gathered by theevaluators . A *product* that has been "evaluated" and "certified" in Europe is thesame as a product that has been "evaluated" in the U.S. A *system* that has been "evaluated" and "certified" in Europe can be considered equivalent to a systemthat has been "certified" in the U.S.

Accreditation

Accreditation, which is the same in Europe as it is in the U.S., is the official administrative approval that is granted to an ADP *system* to process sensitive information in its operational environment. It is based upon anassessment of the system's ability to accomplish its mission while providing sufficient protection features to achieve an acceptable level of risk. The Designated Approving Authority (DAA), typically the individual responsible forthe execution of the mission, specifies the acceptable level of risk. Various government policies and directives mandate certain protection featuresfor each of the security disciplines (e.g., technical, physical, administrative) based on the type of information to be processed and the mission to beaccomplished. Some factors that affect the specification of protection features include:

- range of information (e.g., Unclassified through Top Secret)
- range of users (i.e., clearances)
- intended mode of operation (i.e., dedicated, system high, compartmented, multilevel)
- location of the operation (e.g., is it inside a command center or ina commercial office building?)
- mission and operations concept (e.g., is this a payroll/personnel system or weapons' deployment?)

Protection features can include: physical security (e.g., guards, dogs, fences); administrative and procedural controls; personnel clearance requirements; communication security (e.g., cryptography); emanations security (e.g., TEMPEST control of electromagnetic radiation); and system's hardware and software security design, configuration, and implementation. Anaccreditation decision is made on the basis of a certification by designated technical personnel of the extent to which a system's protection features are adequate. Certification and accreditation are discussed in greater detail in [C&A94].

U.S. Efforts

As described in Module 1, the U.S. identified the need for computer security safeguards in 1967. After several efforts were undertaken during thenext decade, the NCSC (originally called the DoD Computer Security Center) was formed to promote the widespread availability of trusted computer products. Based on those previous efforts, the NCSC produced the first-ever set of computer security requirements (the TCSEC) to be used for buildingtrusted products and for measuring the trust classes of such products. The TCSEC provides the vehicle for vendors to know how to build trusted products and for evaluators to assure acquisition managers and their customers that the trusted products, as developed, provide sufficient security for their intended use. It reduces the need for redundant evaluations that would otherwise be required in support of independent program acquisitions of information protection technology. Other countries have recognized the need for computer security criteria and have leveraged off of the TCSEC to develop their own requirements.

Over the past couple of years, the U.S. has been working to adapt its evaluation criteria and evaluation process. This section describes those efforts, and explains the U.S. export control procedures for trusted products.

Criteria Development

Since its inception as a DoD Standard in 1985, the TCSEC has encountered various complaints about its focus and applicability. In December 1992, NSA collaborated with NIST to produce a new set of draft evaluation criteriacalled the Federal Criteria [FC92]. This criteria, which focuses on integrity and availability in addition to confidentiality, provides generic requirements for the creation of unique sets of information technology building blocks referred to as protection profiles. The Federal Criteria effort has been subsumed by the Common Criteria effort discussed at the end of this module.

Evaluation Processes

In addition to performing evaluations against the TCSEC, NSA also entered into a joint venture with the Defense Intelligence Agency (DIA) in1989 to evaluate compartmented mode workstations (CMWs) against CMWevaluation criteria [CMW87, CMW91]. These CMW criteria introduce "informationlabels" and have some higher-level TCSEC accountability and assurance criteria appearing at class B1 (e.g., B2 trusted path and A1 trusted distribution). DIA has been responsible for producing and disseminating both [CMW87] and [CMW91], and acts as a DAA for some CMW applications. CMW evaluations are included as part of TPEP.

TPEP has been in existence in one form or another since 1984. One of the advantages of this established process is that there is no cost tovendors for the time of evaluators. Another advantage is that much attention is given to consistency among evaluations to ensure a level playing field for vendors. However, there are also disadvantages. NSA has limited evaluation resources and has to be selective concerning the products that it accepts intoTPEP. While the new TPEP evaluation process allows for a much shorter evaluation timescale, the limited resources and the emphasis on consistency among evaluations frequently cause evaluations to take longer than vendorswould like in today's rapidly-changing market climate.

Therefore, under the auspices of NSA's Outreach program, a NIST-operated commercial evaluation scheme is being investigated for lower assurance (B1 and below) products. This initiative, known as the Trust Technology Assessment Program (TTAP), would likely speed up the evaluation process for B1 and below products, but would require vendors to pay for evaluation resources and would require more effort to maintain consistency of evaluations. Since NSA is responsible for classified systems, TPEP would continue to apply to products where higher levels of assurance (B2 andabove) are still necessary. TTAP is intended to be an attractive alternative for vendors who are developing trusted products targeted for the unclassified market (for which NIST is responsible).

Export Controls

Vendors need to be aware of the effect that U.S. export controls could have on their ability to market a trusted product. For reasons of national security, foreign policy, or short supply of certain products, the U.S. controls the export of all goods and technology. Export control responsibilities are divided between two agencies: the Commerce Department administers the export ofcommercial and dual-use products, while the State Department regulates the export of military products. Under both systems, licences are issued before commercial or military products (and technology) can be exported.

Export licences for military items are issued by the State Department in accordance with the International Traffic in Arms Regulation (ITAR). The ITAR contains a U.S. Munitions List, which enumerates what items are controlled under that document. All other goods and services areexported with Commerce Department licenses issued under the Export Administration

Regulation (EAR). The EAR categorizes goods and services in the Commodity Control List.

Commerce (EAR) licenses are usually issued without review outsideof that department. State (ITAR) licenses, on the other hand, are reviewed by the State Department and the DoD. The State Department, with DoD assistance, attempts to determine if exports of military hardware or technology will have a negative impact on the security of the U.S. by increasing the military capabilities of other nations. For more information on export controls contact the following:

Commerce: Exporter Assistance Division
Room 1099D
U.S. Department of Commerce
Washington, D.C 20230

State: Office of Munitions Control SA-6
Department of State
Washington, D.C 20230

The export of computer security (COMPUSEC) products and technology are regulated under both systems, depending on the sophistication of the COMPUSEC product. COMPUSEC items (including hardware, software, and firmware) are exported with ITAR licenses if they contain cryptography {category XIII(b)} or if they have been evaluated under the Department of Defense's TCSEC at class B3 or above {Category XVIII}. All other COMPUSEC products are exported with EAR licenses. The B3 ITAR export requirement also includes the technology on how to design, build, test, and evaluate COMPUSEC products.

This restriction on the export of B3 or A1 products has caused somevendors to purposely target a product for B2 rather than B3 in order to avoid the potential ITAR export restriction. Vendors should be aware of this possibility and plan accordingly when planning the development of a B3 or A1 product.

COMPUSEC ITAR license requests will be reviewed on a case-by-case basis to determine the impact the export would have on national security. Elements taken into consideration are the technology level proposed for export, the country of destination, the use, and the end-user.

International Efforts

Several foreign governments are establishing their own trusted product evaluation programs and fostering the development of international standards. This section presents efforts in the following international arenas: Canada, Europe, the United Kingdom, Australia, and New Zealand.

A source of information on foreign COMPUSEC activities is NSA's Information Systems Security Organization's International Relations Division. The division's mission is to support U.S./Allied military combined operations, develop information security (INFOSEC) foreign policy goals andobjectives , and develop and support bilateral INFOSEC arrangements. Although the

division can offer little assistance in purely commercial COMPUSECventures , they must be contacted whenever foreign governments are involved in COMPUSEC programs that include NSA endorsed products or classified material. The division's staff can assist in the passing of classified documents and in dealing with the security agencies of foreign governments. For more information write:

DIRNSA
Attn.: I11
9800 Savage Rd.
Fort George G. Meade, MD 20755-6000

Canada

The Canadian System Security Centre (CSSC) was established in 1988. Its terms of reference, some of which have now been integrated into the INFOSEC organization of the Computer Security Establishment (CSE), are asfollows:

a. evaluate the hardware and software components of systems to verify or establish a level of confidence in their security;
b. provide information on the security of systems to the government of Canada;
c. direct and conduct research and development of systems' security and systems' security technology; and
d. provide an industry interface to encourage the development of an indigenous capability in the production of secure products.

The Security Policy of the government of Canada specifies that all classified and designated information and assets of the Federal Government are to be safeguarded in an appropriate manner. As a lead agency under this policy, CSE provides an evaluation and development capability on communicationsecurity systems and on computer hardware and software. CSE ensures that relevant information is available to both government and non-government entities on the means available and required to safeguard Government of Canada information and assets.

In order to foster the development of an indigenous INFOSEC capabilityin Canada, CSE introduced several programs to encourage the production of INFOSEC services by Canadian industry. The primary thrust of these programs is to establish flexible industry/government businessrelations whic h foster the timely development of Canadian products meeting CSE security standards and specifications. The resulting products can then be endorsed, evaluated or approved by CSE for government use. These programs are designed to take advantage of Canadian industry's expertise in the design, development and production of telecommunications and computer products. By making classified INFOSEC documentation and CSE technical assistance available to companies which are qualified and interested in producing security products, CSE encourages direct industry involvement and provides a focus for industry development efforts in the design and development of secureproducts for government use. One of the four industrial programs is the Canadian TPEP. The Canadian TPEP was established to increase the production and use of

computer system security components in Canada. The objective of the Canadian TPEP, therefore, is to have products designed, evaluated and produced for use in improving the security of Canadian government information systems.

CSE developed the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), which was published in 1993. The CTCPEC is compatible with its U.S. counterpart, the TCSEC, but is also expanded to include additional criteria on integrity, availability and accountability. CSE has carried out two minicomputer evaluations against the TCSEC and the CTCPEC. At the time of writing, CSE is currently involved in a TCSEC-evaluated operating system port evaluation.

Europe

Significant effort was expended by France, Germany, the Netherlands and the United Kingdom to define and establish a harmonized version of theirseparate national programs. This effort resulted in the Information Technology Security Evaluation Criteria (ITSEC). The ITSEC builds on provenfundamental concepts of the TCSEC and introduces additional requirements, new approaches for specifying security requirements, and new measures of system trust and effectiveness of implementation. It is divided into threeindependent criteria groups: functionality, correctness, and effectiveness. Functionality requirements define the security features of the system. Correctness requirements define levels of assurance. As introduced by the ITSEC, effectiveness is a new measure of assurance; this measure is implied bythe TCSEC and is addressed by U.S. evaluators during the Pre-Evaluation stage of TPEP. Functionality and correctness levels are concerned with aspects of the feature and assurance requirements of the TCSEC. Under the ITSEC, different levels of functionality and correctness can be combined. In the TCSEC, they are already combined in order of increasing functionality and assurance.

The ITSEC allows considerable flexibility in the specification of thesecurity features of a product or system to be evaluated. This flexibilityallows products to be tailored to address perceived threat needs, but also means that it will be more difficult to compare trusted products to one another. Several functionality classes were predefined to specify known functional needs, including a means to provide a mapping from the ITSEC to each of the TCSEC classes. Other predefined classes include systems with requirements for: data and program integrity (e.g., databases), availability (e.g., process control), data integrity during communication, data confidentiality during communication (e.g., cryptographic devices), and network confidentiality and integrity.

The ITSEC correctness requirements incorporate all of the TCSECassurance techniques and introduce many new concepts and approaches to gaining added assurance. More refinement is specified in configuration management, with requirements beginning at the lowest class and increasing with each class. Specific constraints on the compilers that can be used to developsystems is specified for class B1 equivalent and above. There are new requirements that deal with the operational environment, including trusted distribution (at the equivalent of class C1) and initial configuration. Many new requirements are

defined for the development environment, such as source code testing, vulnerability analyses, and object code to source code correspondence.

Effectiveness is an entirely new measure of assurance; it is asubjective analysis and is an integral part of the ITSEC assurance ratings (E1to E6). The analysis focuses on how well a system counters the threat (i.e., strength of mechanism), how well the individual functions work together (i.e., binding analysis), and whether the system users and administrators can bemisled into configuring or using it in an insecure manner (i.e., ease-of-use). Evaluator comments in the final evaluation report of TCSEC evaluations oftentouc h on some of these concerns.

A mapping of specific combinations of predefined functionality andcorrectness levels has been identified which fully satisfies each of the TCSEC classes. The notion is that a product which satisfies one of the specified ITSEC combinations may also meet the requirements of the TCSEC class to which it maps. The reverse is not necessarily true. Since these levels, as discussed above, actually proscribe a superset of the TCSEC requirements, the mapping is ensured in one direction only. There are no guarantees that anything evaluated against TCSEC classes will map back to any predefined ITSEC classes.

Following draft international dissemination to governments and industryfor review and comment, the ITSEC was published in May 1991. This document was followed by the Information Technology Security Evaluation Manual (ITSEM) in 1992. ITSEM defines the detailed work of developersand evaluators in an ITSEC evaluation. Germany has certified severalproducts to ITSEC, but the majority of ITSEC evaluations have taken place in the U.K.

United Kingdom

In 1984, the Communications Electronics Security Group (CESG)assumed responsibility for technical computer security in the U.K. Following the development of U.K. confidence level criteria [CESG89], a number of products and systems were certified against this criteria, which pre-dated ITSEC and ITSEM. CESG joined forces with the U.K.'s Department of Trade and Industry in 1990 to provide a common platform for the evaluation of information technology products and systems for the needs of U.K. government and industry. This initiative became known as the U.K. Information Technology Security Evaluation and Certification Scheme (the Scheme). The Scheme allows international mutual recognition of evaluation results that arebased on the ITSEC.

Under the Scheme, evaluations are commissioned by sponsors who desire to have their products evaluated according to the ITSEC. Both products and systems alike are evaluated to the same criteria and methodology. The U.K. ITSEC Scheme requires that a sponsor finance the complete cost of evaluation, including the time of evaluators. In the case of products, this requirement usually means it is the vendor of the product who pays. The Scheme allows sponsors to enlist the services of evaluators of their choosing and for evaluators to be dedicated to the evaluation for its duration. Sponsors oftencommission evaluators who have specific knowledge of technology so that their training overhead can be reduced and the evaluation can proceed more rapidly. Thus,

the evaluation schedule is largely driven by the sponsor. The U.S. is tracking the progress of this approach as they consider implementing their own commercial evaluation scheme (i.e., TTAP). In particular, the U.S. is tracking the U.K. approach to maintaining consistency of examination from one evaluation to the next. The reader is referred to [UKSP94b] for more information on U.K. ITSEC Scheme evaluations; a copy of [UKSP94b] resides on Dockmaster as **`>udd>CPE>public>uk.epl.new`**.

A number of products have achieved ITSEC certification under the Scheme. Those evaluations which predated the publication of ITSEM were performed in accordance with the Manual of Computer Security Evaluation [CESG88]. Products which have achieved certification against ITSEC comprise operating systems, database management systems, and communications devices. The Scheme is not limited to U.K.-produced products. U.S. products, such as INGRES Enhanced Security and Trusted Oracle 7, have also achieved certification under the Scheme. In the case of Trusted Oracle 7, the U.S. TCSEC evaluation closely mirrored the U.K. ITSEC evaluation. In the opinion of Oracle, the evaluations produced similar results.

Australia and New Zealand

Australia and New Zealand have taken a somewhat different approach than that of the U.S., Canada, and Europe. The amount of trusted system development and acquisition occurring in Australia and New Zealand didnot warrant the expenditure to develop a criteria of their own. Rather thandevelop their own criteria, they have decided to learn about and participate in the development of criteria by the rest of the security world. They willthen understand and adopt these criteria and use the ratings given to trusted systems as input into their own certification/accreditation programs.

ITSEC is the criteria used for Australian and New Zealand evaluations. So far, only communication devices have been evaluated in Australia. Given the number of products requiring evaluation in Australia, the government is currently investigating the establishment of commercial evaluation facilities.

The Defence Signals Directorate in Canberra is the Australian Government agency that is responsible for providing advice and assistance on the automated processing of sensitive information. The Defence Science and Technology Organization (DSTO) is responsible for R&D support of the Australian DoD. DSTO has a group involved in the R&D of trusted computer systems, including both security and safety critical systems.

The Government Communications Security Bureau (GCSB) is responsiblefor computer security in New Zealand. GCSB has evaluated several personal computer products against the ITSEC, including one U.S. product that was of significant national interest but was not being evaluated by any other country.

Towards Common Criteria

At this point in time, mutual recognition of evaluation results has not been achieved. Since 1993, the U.S., U.K., Canada and Europe have been working towards the production of common evaluation criteria known as the Common Criteria. A new, harmonized evaluation process will also be addressed. In time,

these efforts should mean that the results of an evaluation performed inany one of the countries will be accepted by each of the others.

The Common Criteria breaks assurance and functionality into separate components which can be combined and related to threats. The combined groups are referred to as protection profiles. An initial set of functional security criteria for distributed systems has been developed and is beingconsidered for inclusion. For more information on the Common Criteria, contact:

Patricia Toth
NIST
Criteria and Evaluations Group
Building 244, Room 244,
Gaithersburg, MD 20899
(301) 975-5140

Once the Common Criteria is published, the international community plansto participate in a joint evaluation so that evaluation process differencescan be identified and harmonized. The Common Criteria is intended to be backwards compatible with extant criteria: TCSEC, ITSEC and CTCPEC.

Relevant Trusted Product Evaluation Questionnaire Questions

None.

Required Readings

None.

Supplemental Readings

ACAP92 National Computer Security Center, *Assessing Controlled Access Protection*, NCSC-TG-028, Version 1, 25 May 1992.

Berson89a Berson, T. and Lunt, T., "International Orange: Seven Nations Discuss Criteria," *Data Security Letter*, No. 10, June 1989.

This article presents the viewpoints of the members of the panel at the May 1989 IEEE Symposium called International Orange: A Spectrum of Computer Security Criteria. The countries that were represented were: U.S., Sweden, Canada, West Germany, France, England, and Australia. Several of these countries are creating there own evaluation criteria and an effort is being made to try to standardize these.

Berson89b Berson, T. and Lunt, T., "German Criteria Published," *Data Security Letter*, No. 14, December 1989.

This article describes the German Criteria for the Evaluation of Trustworthiness of Information Technology, the German equivalent of the U.S.'s TCSEC.

Berson90 Berson, T. and Lunt, T., "British Publish Draft Criteria," *Data Security Letter*, No. 16, February 1990.

This article describes the British Criteria for computer security evaluation. It is currently five volumes produced by the U.K.'s Commercial Computer Security Centre (CCSC).

Billard90 Billard, B. and Rogers, J., "International Orange: A Spectrum of Computer Security Criteria - An Australian View," *IEEE Cipher Newsletter*, Winter 1990.

This article describes the Australian viewpoint for computer security evaluation. Australia does not plan to develop its own criteria; rather, it plans to understand the U.S. and European criterion and use them for its own purposes.

C&A94 National Computer Security Center, *Introduction to Certification and Accreditation*, NCSC-TG-029, Version 1, January 1994.

ENV85 Computer Security Center, *Guidance for Applying the DoD TCSEC in Specific Environments*, CSC-STD-003-85, June 1985.

Lunt90 Lunt, T., "International Orange: Six Nations Report Progress on Criteria," *Data Security Letter*, No. 19, July 1990.

This article presents the viewpoints of the members of the panel at the May 1990 IEEE Symposium called International Orange II. The countries that were represented were: U.S., Sweden, Canada, West Germany, Great Britain, and Australia. Three countries have published draft criteria, and four of the countries have developed a Harmonized Criteria.

Other Readings

Brown88 Brown, R.L., "Interdependence of Evaluated Subsystems," *Proceedings of 11th National Computer Security Conference*, October 1988.

Provides guidance to DAAs who must determine that a proposed computer system may be used to process sensitive information. This guidance is specific to entire trusted computer systems and does not address the topic of trusted subsystems running on otherwise untrusted computer systems.

CESG88 Communications Electronics Security Group, *Computer Security Manual A - Manual of Computer Security Evaluation*, Issue 1.0, December 1988.

CESG89 Communications Electronics Security Group, *Computer Security Memorandum No. 3, UK System Security Confidence Levels*, Issue 1.1, February 1989.

CMW87 Defense Intelligence Agency, *Security Requirements for System High and Compartmented Mode Workstations*, DDS-2600-5502-87, November 1987.

CMW91 Defense Intelligence Agency, *Compartmented Mode Workstation Evaluation Criteria*, DDS-2600-6243-91, Version 1, June 1991.

CTCPEC93 Canadian System Security Centre, *The Canadian Trusted Computer Product Evaluation Criteria*, Version 3.0e, January 1993.

FC92 National Institute of Standards and Technology & National Security Agency, *Federal Criteria for Information Technology Security, Volume 1, Protection Profile Development*, Version 1.0, December 1992.

ITSEC91 Commission of the European Communities, *Information Technology Security Evaluation Criteria (ITSEC)*, Version 1.2, 28 June 1991.

ITSEM93 Commission of the European Communities, *Information Technology Security Evaluation Manual (ITSEM)*, Version 1.0, September 1993.

UKSP91 U.K. Certification Body, *Licensing of Commercial Licenced Evaluation Facilities*, UKSP-02, Issue 1.0, 1 March 1991.

UKSP94a U.K. Certification Body, *Description of the Scheme*, UKSP-01, Issue 2.0, April 1994.

UKSP94b U.K. Certification Body, *Certified Products List*, UKSP-06, September 1994.